UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/491,727	01/27/2000	David M. Austin	AUZ-001 P	8984

7590 11/12/2003

Wesley L Austin esq
1987 South Bluebell drive
Bountiful, UT 84010

EXAMINER
ALI, AHMEDUR R

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/12/2003

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/491,727	AUSTIN ET AL.	
	Examiner	Art Unit	
	Ahmedur Ali	2131	

-- The MAILING DATE of this communication appears on the cover she t with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. The application has been examined. Claims 1-31 are pending in this Office Action.

Drawings

2. The drawings are objected to by the draftsperson. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claim 1-32 are rejected under 35 U.S.C. 102(a) as being anticipated by Drake (U.S. Patent No. 6,006,328). With respect to claim 1, Drake teaches a system for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), the system comprising:

accessing instructions that access observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

reading instructions that tread memory of the computer system to obtain memory data (see col. 4, lines 47-65; col. 6, lines 10-20)

comparing instructions that compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system (see col. 6, lines 5-48);

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer system (see col. 6, lines 5-48); and

outputting instructions that obtain the results and provide the results for a user (see col. 4, lines 47-65; col. 6, lines 5-48).

7. Claim 2 is rejected as above in rejecting claim 1, wherein the reading instructions read the memory of the computer system by querying the operating system of the computer system for the tasks running and by examining task information provided by the operating system (see col. 3, lines 32-67).

8. Claim 3 is rejected as above in rejecting claim 1, wherein the outputting instructions provide the results to a user through a graphical user interface (see col. 9, lines 8-14; col. 10, lines 12-16).

9. Claim 4 is rejected as above in rejecting claim 1, wherein the reading instructions read the memory of the computer system by querying the file system of the computer system for the files located on storage media and by examining file information provided by the file system (see col. 6, lines 7-20).

10. Claim 5 is rejected as above in rejecting claim 1, wherein the reading instructions read the memory of the computer system by opening a file located on storage media and by examining contents of the file (see col. 6, lines 10-20).

11. Claim 6 is rejected as above in rejecting claim 1, wherein the observer data includes data descriptive of a plurality of observer programs and wherein the system compares the observer

data with the memory data to determine whether any known observer program is present (see col. 6, lines 7-48).

12. Claim 7 is rejected as above in rejecting claim 1, further comprising countermeasure instructions wherein the countermeasure instructions alter the operation of the observer program (see col. 3, lines 46-52).

13. Claim 8 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering observer program configuration data (see col. 4, lines 47-65; col. 8, lines 3-12).

14. Claim 9 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering a file on the computer system (see col. 7, lines 12-23; col. 8, lines 3-12).

15. Claim 10 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering reporting data generated by the observer program (see col. 5, lines 20-34; col. 7, lines 53-67 to col. 8, lines 1-12).

16. Claim 11 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by replacing reporting data generated by the observer program (see col. 5, lines 38-62).

17. Claim 12 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by replacing a file of the observer program (see col. 5, lines 20-34).

18. Claim 13 is rejected as above in rejecting claim 1, wherein the observer data includes data descriptive of observing activity typical of observing programs and

wherein the system compares the observer data with the memory data to determine whether any known observer program is present (see col. 6, lines 5-48).

19. Claim 14 is rejected as above in rejecting claim 1, further comprising the observer data, wherein the observer data includes a list of files and modules that are part of the observer program software, and wherein the reading instructions read the memory of the computer system by querying the operating system of the computer system for the tasks running and by examining task information provided by the operating system, and wherein the reading instructions also read the memory of the computer system by querying the file system of the computer system for the files located on storage media and by examining file information provided by the file system, and wherein the outputting instructions provide the results to a user through a graphical user interface (see col. 3, lines 32-57; col. 4, lines 47-65; col. 6, lines 5-48).

20. Claim 15 is rejected as above in rejecting claim 1, wherein the system is made available over a computer network through a web site (see col. 13, lines 28-34).

21. With respect to claim 16, Drake teaches a system for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), the system comprising:

means for accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

means for reading memory of the computer system to obtain memory data (see col. 4, lines 47-65; col. 6, lines 10-20).

means for comparing the observer data with memory data to determine whether the observer program is present on the computer system (see col. 6, lines 5-48);

means for generating results from the comparison, wherein the results generated indicate whether the observer program is present on the computer system (see col. 6, lines 5-48); and

means for outputting the results for a user see col. 4, lines 47-65; col. 6,lines 5-48).

22. With respect to claim 17, Drake teaches a method for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), the method comprising the steps of:

accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

reading memory of the computer system to obtain memory data (see col. 4,lines 47-65; col. 6, lines 10-20);

comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system (see col. 6, lines 5-48);

generating results from the reading and comparing, wherein the results generated indicate whether the observer program is present on the computer system (col. 6, lines 5-48); and

outputting the results for a user (see col. 4, lines 47-65; col. 6, lines 5-48).

23. With respect to claim 18, Drake teaches a computer-readable medium containing instructions for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), wherein the instructions comprise executable instructions for implementing a method comprised of the steps of:

accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3,lines 32-67);

reading memory of the computer system to obtain memory data (see col. 4,lines 47-65; col. 6, lines 10-20);

comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system (see col. 6, lines 5-48);

generating results from the reading and comparing, wherein the results generated indicate whether the observer program is present on the computer system (see col. 6, lines 5-48); and

outputting the results for a user (see col. 4, lines 47-65; col. 6, lines 5-48).

24. Claim 19 is rejected as above in rejecting claim 18, wherein the computer-readable medium is a data transmission medium (see col. 13, lines 27-33).

25. With respect to claim 20, Drake teaches a system for altering the operation of an observer program on a computer system, the system comprising (see abstract; col. 3, lines 32-44; col. 4, lines 47-65):

accessing instructions that access observer information, the observer information including data descriptive of the observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3,lines 32-67);

reading instructions that read memory of the computer system to obtain files relating to the observer program (se col. 4, lines 47-65; col. 6, lines 10-20);

altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

26. Claim 21 is rejected as above in rejecting claim 20, comprising an observer detection program (see col. 3, lines 32-44).

27. Claim 22 is rejected as above in rejecting claim 20, further comprising inputting instructions that display to a user options regarding the altering and that take input from the user relating to

the options (see col. 11, lines 30-46).

28. Claim 23 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by altering observer program configuration data (see col. 4, lines 47-67 to col. 5, lines 1-14; col. 6, lines 21-31).

29. Claim 24 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by altering a file on the computer system (see col. 4, lines 47-67 to col. 5, lines 1-14)

30. Claim 25 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by altering reporting data generated by the observer program (see col. 4, lines 47-65; col. 5, lines 37-58).

31. Claim 26 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by replacing reporting data generated by the observer program (see col. 4, lines 47-65; col. 5, lines 37-58).

32. Claim 27 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by replacing a file of the observer program (see col. 4, lines 47-65; col. 5,lines 37-58).

33. Claim 28 is rejected as above in rejecting claim 20, wherein the system is made available over a computer network through a web site (see col. 13, lines 27-33).

34. With respect to claim 29, Drake teaches a system for altering the operation of an observer program on a computer system (see abstract; col. 3, liens 32-44; col. 4, lines 47-65), the system comprising:

means for accessing observer information, the observer information including

data descriptive of the observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

means for reading memory of the computer system to obtain files relating to the observer program (see col. 4, lines 47-67; col. 6, lines 10-20); and

means for altering a file relating to the observer program such that the operation of the observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

35. With respect to claim 30, Drake teaches a method for altering the operation of an observer program on a computer system (see abstract; col. 3, lines 32-44; col. 4, lines 47-65), the method comprising the steps of:

accessing observer information, the observer information including data descriptive of the observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

reading memory of the computer system to obtain files relating to the observer program (see col. 4, lines 47-67; col. 6, lines 10-20) and

altering a file relating to the observer program such that the operation of the observer program is; changed (see col. 5, lines 42-62; col. 8, lines 3-12).

36. With respect to claim 31, Drake teaches a computer-readable medium containing instructions for altering the operation of an observer program on a computer system, wherein the instructions comprise executable instructions for implementing a method comprised of the steps of:

accessing observer information, the observer information including data descriptive of the observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

reading memory of the computer system to obtain files relating to the observer program (see col. 4, lines 47-65; col. 6, lines 10-20); and

altering a file relating to the observer program such that the operation of the observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

37. Claim 32 is rejected as above in rejecting claim 31, wherein the computer-readable medium is a data transmission medium (see col. 13, lines 27-33).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Tajalli et al. (U.S. Patent No. 5,361,359) disclose a system and method for controlling the use of a computer)

Rowland (U.S. Patent No. 6,405,318) discloses an intrusion detection system.

Cross et al. (U.S. Patent No. 6,154,775) disclose methods and apparatus for a computer network firewall with dynamic rule processing with the ability to dynamically alter the operations of rules.

Knowlson (U.S. Patent No. 6,108,786) discloses a monitor network bindings for computer security.

Kuo et al. (U.S. Patent No. 6,230,288) disclose a method of treating whitespace during virus detection.

Chen et al. (U.S. Patent No. 5,832,208) disclose an anti-virus agent for use with databases and mail servers.

Wells (U.S. Patent No. 6,338,141) discloses a method and apparatus for computer virus detection, analysis, and removal in real time.

Wygodny et al. (U.S. Patent No. 6,282,701) disclose a system and method for monitoring and analyzing the execution of computer programs.

Chambers (U.S. Patent No. 5,398,196) discloses a method and apparatus for detection of computer viruses.

Dunne (U.S. Patent No. 4,140,953) discloses real time program modification apparatus.

Chen et al. (U.S. Patent No. 6,327,700) disclose a method and system for identifying instrumentation targets in computer programs related to logical transactions.

Chi (U.S. Patent No. 5,978,917) discloses a detection and elimination of macro viruses.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmedur Ali whose telephone number is 305-4667. The examiner can normally be reached on 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 305-3900.

ara

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100